UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,547	10/14/2003	J. Scott Carr	P0869	3480

23735 7590 10/21/2008

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
10/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/686,547	CARR ET AL.	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-20,25 and 27-29* is/are pending in the application.

4a) Of the above claim(s) *13, 26, and 30-51* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-20,25 and 27-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12, 14-20, 25, and 27-29 are pending.

Claims 13 and 26 have been cancelled.

Claims 21-24 and 30-51 have been withdrawn.

2. The 112, 2nd paragraph rejection for claim 25 is withdrawn due to the current amendment.

Response to Arguments

3. Applicant's arguments with respect to claims 1-12, 14-20, 25, and 27-29 have been considered but are moot in view of the new ground(s) of rejection.

Examiner traverses the argument on pg.13, that Wu does not verify an age level of the document. Wu's invention is mainly about verifying the authenticity of an electronic document or article such as identification cards, passports, credit cards, etc. (col.6, lines 5-16). Wu includes personal particulars includes person's age or birth date, blood group, and height (col.7, lines 20-23 and col.8, lines 1-3). Wu teaches using encrypted information and seeds (col.2, lines 5-22) for generating a watermark is obtained from a portion of an article or document (col.7, lines 35-37 and col.8, lines 4-7). The biometrics data or information and other appending information alone or together can be provided as input that will identify invariant features. The invariant features have a size of a few hundred bites which is given as the claimed identification document comprising plural bits (col.11, lines 5-18) and the watermark which is reduced-bit representation that was generated from a portion of the document reads on the claimed generating a reduced-bit representation of the

received information carried by the document. Therefore, Wu reads on comparing data corresponding to the second field with the reduced-bit representation to verify an age level of the document.

Claims 27-29 are also rejected due to their dependency.

Examiner traverses the argument of claim 1 on pg.13-14, that Wu does not discuss verifying a bearer's age when second digital data and the third digital data correspond. Wu discloses the foregoing authentication or verification process is carried out until all portions of the article are checked where portions are explained (below) in the office action (col.9, lines 1-22). Thus, Wu reads on the claim 1. Claims 2-11 are also rejected by virtue of their dependency.

Examiner traverses the argument of claim 12 on pg.14, that Wu does not protect the anonymity of the person in possession of the identification document. Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Innuendo that Wu does not discuss anonymity of the owner/person's identification document, Moskowitz discloses this limitation. Moskowitz discloses anonymity and legacy relationships may be maintained (Moskowitz - col.20, line 60 and col.38, lines 3-8). Therefore, Wu and Moskowitz combination reads on claim 12. Claims 14-20 are also rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 25 and 27-29 are rejected under 35 U.S.C. 102(e) as being anticipated over Wu, et al. (US 6,748,533).

As per claim 25:

Wu discloses a method comprising:

receiving optical scan data that is associated with an identification document (col.3, lines 29-42 and Fig.6), the identification document comprising plural-bits of data carried by the identification document (col.7, lines 35-37 and col.11, lines 5-18), wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document (col.3, lines 5-18 and col.6, lines 48-64) and the second field corresponding to an age or age level of the bearer of the identification document; (col.7, line 25 – col.8, line 3)

decoding the optical scan data to recover corresponding to at least the second field; (col.1, lines 45-53)

receiving information carried by the document (col.2, lines 5-22 and col.8, lines 4-7), separate from the data corresponding to at least the second field- and generating a reduced-bit representation of the received information; and (col.4, lines 20-27 and col.11, lines 20-40)

comparing data corresponding to the second field with the reduced-bit representation to verify an age level of the document, (col.5, lines 1-34 and col.9, lines 1-22)

wherein neither the data corresponding to the second field nor the reduced-bit representation, betray the identity of the ~~authorized~~ bearer of the identification document. (col.12, lines 1-9 and 44-67 and col.13, lines 15-27)

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed reduced-bit representation can broadly be interpreted as a watermark representation. Wu teaches using encrypted information and seeds (col.2, lines 5-22) for generating a watermark is obtained from a portion of an article or document (col.7, lines 35-37 and col.8, lines 4-7). The biometrics data or information and other appending information alone or together can be provided as input that will identify invariant features. The invariant features have a size of a few hundred bites which is given as the claimed identification document comprising plural bits (col.11, lines 5-18). Wu further discloses the method of generating a watermark involves this information is encrypted and a random pattern is generated (col.4, lines 20-27 and col.11, lines 20-40). Thus, the watermark which is reduced-bit representation that was generated from a portion of the document reads on the claimed generating a reduced-bit representation of the received information carried by the document. Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28) such as an identification, name of the person, fingerprint, and personal particulars such as age and height (col.7, line 65 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22).

As per claim 27: See Wu on col.7, lines 35-37 and col.4, lines 48-55; discussing the method of claim 26, further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

As per claim 28: See Wu on col.8, lines 63-67; discussing the method of claim 26, further comprising printing the data corresponding to the second field to evidence examination of the identification document.

As per claim 29: See Wu on col.1, lines 45-50; discussing the method of claim 25, wherein said receiving information carried by the document comprises receiving data corresponding to at least one of data generated by a barcode scanner, optical character recognizer, manual entry or watermark decoder.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-12 and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wu, et al. (US 6,748,533) in view of Moskowitz (US 7,159,116)

As per claim 1:

Wu discloses a method of verifying an age of a bearer of a document, said method comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from [*auxiliary data steganographically embedded in the document*]; (col.7, line 65 – col.8, line 3)

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from [*auxiliary data steganographically embedded in the document*]; (col.3, lines 5-25 and col.6, lines 28-55)

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and (col.10, lines 53-67 and col.11, lines 5-13)

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age (col.7, lines 20-28), and ii) the second digital data and the third digital data correspond. (col.5, lines 14-33 and col.9, lines 1-22)

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed auxiliary data steganographically embedded in the document is in the form of a watermark embedded on the article, document, or passport because the watermark like auxiliary data steganographically embedded is invisible for protection against forgery (col.2, lines 45-48 and col.5, lines 14-33). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28) such as an identification, name of the person, fingerprint, and personal particulars such as age and height (col.7, line 65 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67 and col.11, lines 5-13) and the authentication/verification process is carried out until all portions of the article are checked (col.9, lines 1-22). Wu discloses embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Thus, Wu obviously suggests auxiliary data steganographically embedded in the document by capturing digital data such as biometric samples, storing the person's age and biometrics, and embedding an invisible watermark

onto a document (col.6, lines 28-55 and col.7, line 65 – col.8, line 3). However, Wu did not clearly discuss auxiliary data steganographically embedded in the document.

Moskowitz discloses the invention for enhancing trust in transactions between plurality of parties where the use of highly-secure steganographic computer processing means for data identification, authentication, and transmission, such that confidence in the transaction components is enhanced (see abstract). Moskowitz explains that encryption and secure digital watermarking (e.g. steganographic ciphering) offer tools for determining data integrity, authenticity, and confidence (col.17, lines 60-67). Further, Moskowitz discusses the application of steganographic ciphers enables an "optimized envelope" for securely inserting, detecting, and protecting informational signals, or data, or digital watermarks (predetermined messages) in a given digitized sample stream (col.20, lines 62-67). Images, medical or human-conditioned based, audio signals, video multimedia, virtual reality, etc. all provide rich media information in which to enhance the security of any embodiment contemplated by the present invention. Combinations of multidimensional media for varying ciphering options as well as steganographic embedding are also contemplated as means for ensuring computational complexity to any unauthorized user. Steganographic-mapping (watermarking) or transfer functions (scrambling or "chaffing") may be combined with encryption ciphers as a means for making each unique implementation or tangible device serialization or personalization of a method for engaging in trusted transactions, high risk, information-intensive or sensitive decision (col.31, lines 49-65). Moskowitz discloses certification authorities having the ability to determine the authenticity of data and may be further bound by geographical or age basis to verify (col.37, lines 8-12 and col.38, lines 27-34). Hence, Moskowitz teaches auxiliary data steganographically embedded in the document involving biometric and age data.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Wu's embedding an invisible watermark (Wu on col.2, lines 45-48 and col.5, lines 14-33) with Moskowitz teaching steganographically embedded in the document because steganographic embedding are also contemplated as means for ensuring computational complexity to any unauthorized user and that steganographic-mapping (watermarking) may be combined with encryption ciphers as a means for making each unique implementation or tangible device serialization or personalization of a method for engaging in trusted transactions, high risk, information-intensive or sensitive decision (Moskowitz – col.31, lines 49-65) such that confidence in the transaction components is enhanced (Moskowitz – see abstract).

As per claim 2: See Moskowitz on col.31, lines 49-65; discussing the method of claim 1, further comprising interrogating a data repository with the biometric indictor to obtain digital data being obtained from auxiliary data steganographically embedded in the document because

As per claim 3: See Wu on col.7, line 65 – col.8, line 3**;** discussing the method of claim 2, further comprising interrogating the data repository with the age indictor to obtain the first digital information.

As per claim 4: See Wu on col.3, lines 5-15 and col.7, line 20-67 ; discussing the method of claim 2, wherein the second digital data comprises a biometric template associated with the bearer.

As per claim 5: See Wu on col.7, line 20– col.8, line 3**;** discussing the method of claim 4, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 6: See Wu on col.7, line 55 – col.8, line 3; discussing the method of claim 1, wherein the third digital data is received through a network.

As per claim 7: See Moskowitz in abstract; discussing the method of claim 6, wherein the

network comprises the internet.

As per claim 8: See Wu on col.7, line 55 – col.8, line 3**;** discussing the method of claim 1, wherein the biometric indicator comprises a biometric template.

As per claim 9: See Wu on col.7, line 55 – col.8, line 3; discussing the method of claim 8, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 10: See Moskowitz on col.6, lines 5-14; discussing the method of claim 1, wherein the third digital data further comprises a timestamp.

As per claim 11: See Wu on col.7, lines 20-67 and col.11, lines 5-18**;** discussing the method of claim 4, wherein the auxiliary data comprises plural bits of data and wherein the biometric indicator and the age indicator comprise the same plural bits.

As per claim 12:

Wu discloses a method of anonymously verifying an age or characteristic associated with a person, the person being in possession of an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person, said method: (see Figs.1 and 6)

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor; (col.10, lines 53-67 and col.11, lines 5-13)

decoding the scan data to obtain the first set of information included in the digital watermark, the first set of information *[including a concatenated string of data]* comprising age indicator and

additional data, wherein the digital watermark is embedded in the identification document (col.4, lines 28-30 and col.5, lines 10-33) through hidden changes to data representing one or more items carried by the identification document; and (col.3, lines 5-25 and col.6, lines 28-55)

determining, based on the first set of information, the person's age or age level, wherein said act of determining protects the anonymity of the person in possession of the identification document. (col.7, lines 20-28 and col.7, line 65 – col.8, line 3)

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28) such as an identification, name of the person, fingerprint, and personal particulars such as age and height (col.7, line 65 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67 and col.11, lines 5-13) and the authentication/verification process is carried out until all portions of the article are checked (col.9, lines 1-22). Wu discloses embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other unauthorized modification (col.12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col.8, lines 28-30 and col.9, lines 43-45). However, Wu did not clearly discuss the watermark containing information including concatenated string of data.

Moskowitz discloses the invention for enhancing trust in transactions between plurality of parties where the use of highly-secure steganographic computer processing means for data identification, authentication, and transmission, such that confidence in the transaction components is

enhanced (see abstract). Moskowitz explains that encryption and secure digital watermarking (e.g. steganographic ciphering) offer tools for determining data integrity, authenticity, and confidence (col.17, lines 60-67). Steganographic-mapping (watermarking) or transfer functions may be combined with encryption ciphers as a means for making each unique implementation or tangible device serialization or personalization of a method for engaging in trusted transactions, high risk, information-intensive or sensitive decision (col.31, lines 49-65). Moskowitz discloses a way to generate a unique ID is with a one-way hash function where the hash result may be concatenated on the digitized, value added information which is the subject of a transaction (col.10, lines 25-28). Moskowitz discloses to provable manufacture secure devices may be accomplished with such protocols as digital time stamping or digital watermarking where instead of time, other predetermined data is concatenated with data for provably establishing ownership over the device (col.22, lines 51-60).

Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col.2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. Innuendo that Wu does not discuss anonymity of the owner/person's identification document, Moskowitz discloses this limitation. Moskowitz discloses anonymity and legacy relationships may be maintained (Moskowitz - col.20, line 60 and col.38, lines 3-8).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Wu's embedding an invisible watermark (Wu on col.2, lines 45-48 and col.5, lines 14-33) with Moskowitz

teaching the watermark containing information including concatenated string of data because to transparently and provably establishing ownership over secure devices (col.22, lines 51-60) and to generate a unique ID with a one-way hash function (col.10, lines 25-28).

As per claim 13: Cancelled

As per claim 14: See Wu on col.7, line 53 – col.8, line 3; discussing the method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

As per claim 15: See Wu on col.8, lines 22-30; discussing the method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

As per claim 16: See Wu on col.1, lines 44-52 and col.8, lines 22-30; discussing the method of claim 14, further comprising computing a hash of the third set of information that is printed on the identification document, decoding the second set of information that is embedded in the identification document to obtain the embedded hash, and comparing the computed hash and the embedded hash to determine authenticity of the document.

As per claim 17: See Wu on col.7, lines 20-27 and Moskowitz on col.6, lines 1-13; discussing the method of claim 12, further comprising storing at least a portion of the first set of information in at least one of a list, electronic memory circuits and a data record, wherein the stored portion of the first set of information serves as an audit clue to evidence that the identification document has been examined.

As per claim 18: See Wu on col.11, lines 15-18 and see FIG.6; discussing the method of claim 17,

wherein the first set of information comprises two or more random bits.

As per claim 19: See Wu on col.7, lines 20-30; discussing the method of claim 18, wherein the first set of information comprises a date of birth.

As per claim 20: See Wu on col.11, lines 15-18 and see FIG.6 and on col., lines and col., lines; discussing the method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2435